



The North Carolina Office of the State Controller

Internal Controls Over Payroll Processes and IT General Controls

April 6, 2011

**David McCoy
State Controller**



Introduction

Statewide Internal Control Program

Enhancing
Accountability in
Government through
Leadership and
Education





Introduction

Administrative Items

- Phones have been muted. For questions during the webinar or for technical assistance – email Jennifer Trivette at jennifer.trivette@osc.nc.gov.
- Course materials have been provided in advance.
- Qualifies for up to 2 hours of CPE.





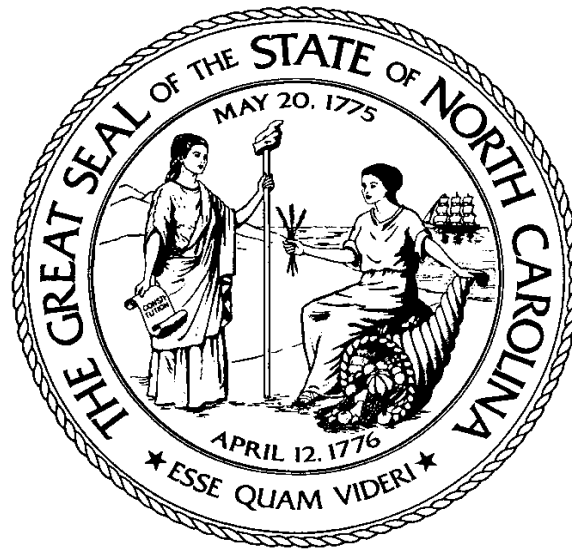
Introduction

Agenda

<u>Estimated Time</u>	<u>Topic</u>
9:30 – 9:35	<i>Welcome and Introduction – Ben McLawhorn</i>
9:35 – 10:00	<i>Overview of Related Audit Findings – Carol Smith and Michael Burch</i>
10:00 – 10:10	<i>Overview of Internal Controls and Risk – Jennifer Trivette</i>
10:10 – 10:20	<i>Implementing Internal Controls over Payroll Processes – Amanda Williams</i>
10:20 – 10:30	<i>Identifying the Risk in Each Payroll Process - What Could Go Wrong? – Amanda Williams</i>
10:30 – 10:45	<i>How Payroll Control Weaknesses Could Lead to an Opportunity for Fraud? – Amanda Williams</i>
10:45 – 10:55	<i>Nature of Controls at the Transaction Level – Wynona Cash</i>
10:55 – 11:05	<i>Considering IT General Controls – Wynona Cash</i>
11:05 – 11:15	<i>Understanding IT General Controls – Wynona Cash</i>
11:15 – 11:20	<i>How IT General Controls Weaknesses Could Lead to Fraud – Wynona Cash</i>
11:20 – 11:30	<i>Key Take-Aways & Questions – Ben McLawhorn</i>



Office of the State Auditor (OSA)



Carol Smith, CPA
Financial Audit Manager

Office of the State Auditor Payroll Findings



Internal Controls for Payroll Findings Related to:

- State Agency Audits/CAFR Audits for 2009 and 2010
- University Financial Audits for 2009 and 2010
- College Financial Audits for 2009 and 2010
- Fiscal Control Audits for July thru December 2008 / February 2009

Office of the State Auditor

Payroll Findings



State Agencies – Financial Statement Findings

- Payroll time Entries Not Verified – control procedures to ensure accuracy of payroll time entries were not followed – finding reported for 2009 and 2010
- Monthly bank balance in the State's payroll account not fully reconciled since January 2008 – monthly differences accumulated to make payroll record reconcile to bank each month

Office of the State Auditor

Payroll Findings



State Agencies – Single Audit Findings

- Improper Allocation of Salaries to Fund Sources – time keeping system allocated payroll to grants based on an initial estimate of time each employee will spend on the grant – actual time is tracked through another system and journal entries are made to reallocate the payroll charges to the proper grant – timekeeping system and time and activity reporting system were not reconciled (2010)
- Salaries not Allocated to Grants Based on Time and Attendance Records (2009)

Office of the State Auditor

Payroll Findings



State Agencies – Single Audit Findings (cont.)

- Personnel Costs Charged to Grant in Error – Controls not in place to ensure that only allowable personnel costs were charged to grant. Part of two employees' salaries and benefits were charged to incorrect grant. (2009)
- Deficiencies in Cash Management Procedures resulted in drawdown of excess funds for Payroll
- System access was not terminated immediately upon employees leaving employment. Risk of overpayment.

Office of the State Auditor

Payroll Findings



Colleges/ Universities

- Inappropriate Information Systems Access to payroll and human resource areas (2009 – 7 Colleges/ 2010 - 2 Colleges) (2009 – 3 universities)
- Access to information systems not properly terminated for separated employees – 2009 - 1 university

Office of the State Auditor

Payroll Findings



Fiscal Control Audits – July 2008 thru December 2008/ February 2009

- Deficiencies in internal control over administration of personnel and payroll.
- Noncompliance with State policies and increased risk of errors in compensation paid to employees.
- Manual timesheets not consistently signed by employees or approved by supervisor.
- Varying time periods for accumulating an employee's time worked compounded difficulty in determining the accuracy of compensation paid.
- Payroll reconciliations not complete.

Office of the State Auditor

Payroll Findings



Fiscal Control Audits – July 2008 thru December 2008/ February 2009 (cont.)

- Inadequate segregation of duties over payroll and human resources
- Payroll disbursing account not reconciled
- Lack of authorization over employee pay rates
- University paid salaries without having an authorized funding source in place and also paid salaries from source authorized. Seven employees continued to be paid after the federal funding for their position was no longer available. One employee paid from source not approved by OSP.

Office of the State Auditor

Payroll Findings

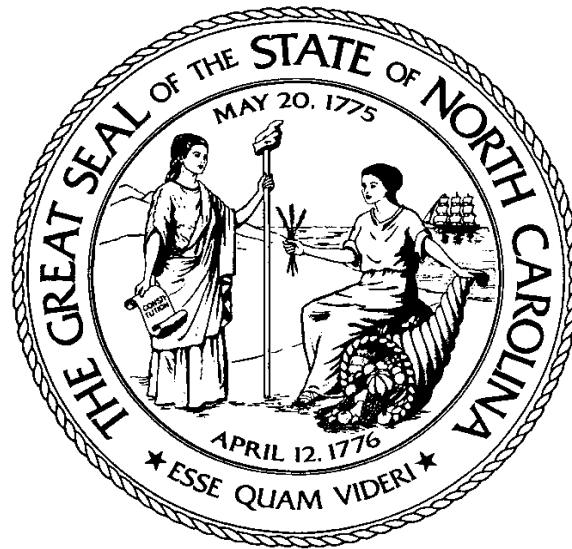


Fiscal Control Audits – July 2008 thru December 2008/ February 2009 (cont.)

- Failure to monitor and reconcile reported variances in payroll reports.
- Inadequate controls over salary advances.
- Several employees erroneously paid for overtime and one received inappropriate longevity payment.
- Inadequate controls over employee separations – risk of errors in final payments
- Inconsistencies with compensated absences reports



Office of the State Auditor (OSA)



Michael E Burch, CPA, CISA
IS Audit Manager



Office of the State Auditor IT Findings

Objective

To highlight the most common findings found in IS Audits for the last two years.



Office of the State Auditor IT Findings

Passwords & User Accounts

- Expiration period for privileged users' passwords are not in compliance with the Statewide Security Manual's requirement of 60 days.
- Default user accounts for applications not removed or default passwords for these accounts not changed.



Office of the State Auditor IT Findings

Access Rights

- Individuals have been granted more access rights than necessary to perform their job duties.
- Access rights for terminated employees not removed timely.
- Access rights for employees changing positions not changed timely or not changed to reflect new job responsibilities.



Office of the State Auditor IT Findings

Review of Access Rights

- Access rights not reviewed in compliance with the Statewide Security Manual.
 - Twice a year for regular users
 - Quarterly for privileged users
- Review of access rights not performed by individuals other than security officers.
- Review of access rights not documented by individual performing review.



Office of the State Auditor IT Findings

Back-Ups

- Back-up tapes stored on-site in media safes rather than at off-site locations.
- Replication Servers used for back-ups are located on-site with no back-ups stored at an off-site location.



Office of the State Auditor IT Findings

Disaster Recovery Plans

- Disaster Recovery Plans are not updated to include new applications or to reflect changes in Information Technology environment, such as moving from mainframes to servers.
- Disaster Recovery Plans not tested or no documentation of testing when recovery from back-up tapes is used as a test.



Office of the State Auditor IT Findings

Statewide Security Manual

- Agencies and Universities not in compliance with the Statewide Security Manual standards.
- Universities have not developed their own security standards in place of the Statewide Security Manual standards.



Office of the State Auditor IT Findings

SAS 70 or SOC Reports

SAS 70 or Service Organization Controls (SOC) reports have not been obtained for service providers to document controls for financial reporting or controls related to compliance and operations.



Office of the State Auditor IT Findings

Reconciliation of Data Transfers

Data transferred between applications is not reconciled by users to ensure completeness and accuracy of data transferred.



Office of the State Auditor IT Findings

Security Governance

- Management have not provided policies, procedures, standards, and guidance for system administrators in the configuration of security for servers, databases, and network devices.
- Systems not secured or hardened before being placed on network.



Office of the State Auditor IT Findings

Security Baselines

- No baselines for security settings for servers, databases, and network devices on the network.
- Current security settings for servers, databases, and network devices not compared to baselines to identify unauthorized or unapproved changes.



Office of the State Auditor IT Findings

Patches and Change Control

- Patches for servers' operating systems and databases not installed timely.
- No change control methodology for servers, databases, and network devices.



Office of the State Auditor IT Findings

Passwords for Network Devices

- Network devices default user accounts not removed or default passwords for these accounts not changed.
- Passwords for network devices not changed on a regular schedule.



Office of the State Auditor IT Findings

Network Printers, Copiers, & Scanners

Systems Administrators are unknowingly introducing vulnerabilities into the state networks by placing unsecured network printers, copiers, and scanners onto the State's Network.



Office of the State Auditor IT Findings

Network Vulnerability Assessments

Network vulnerability assessments including penetration testing not performed.



Overview of Internal Controls and Risk



Overview of Internal Controls and Risk

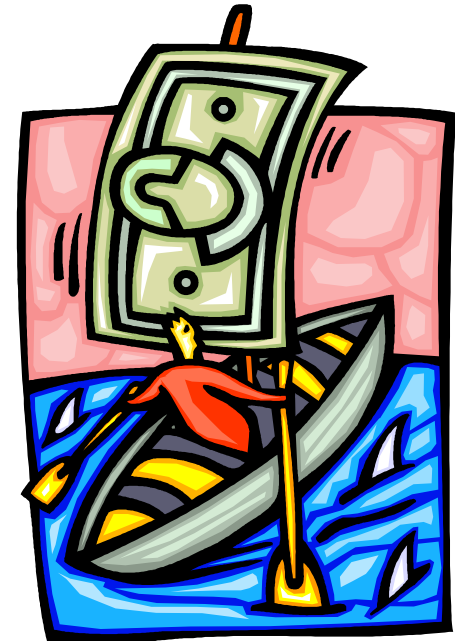
Overview

- What is Internal Control?
- Internal Control Activities
- What is Risk?
- What Could Go Wrong?
- Types and Nature of Controls
- Balancing Risk and Control



Overview of Internal Controls and Risk

A control is any action taken to mitigate or manage risk and increase the probability that the organization's processes will achieve its goal or objectives.





Overview of Internal Controls and Risk

What is Internal Control?

Internal control is a process, effected by an entity's governing body, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Effectiveness and efficiency of operations



Overview of Internal Controls and Risk

Why do we need internal controls?

- Internal controls provide a foundation for accountability.
- Internal controls are the checks and balances that help managers detect and prevent problems.



Overview of Internal Controls and Risk

Internal Control Activities:

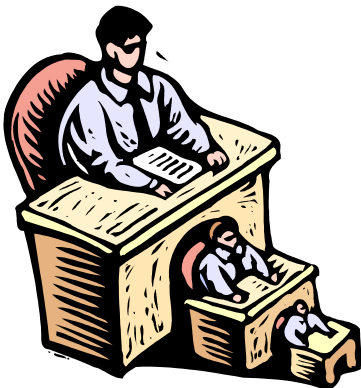
- Adequate segregation of duties
- Proper authorization of transactions and activities
- Adequate documentation and records
- Physical control over assets and records
- Independent checks on performance



Overview of Internal Controls and Risk

Adequate Segregation of Duties

- Requires different individuals be assigned responsibility for different elements of related activities.
- For example, responsibilities for payroll approval, data entry, and disbursement functions should be segregated and assigned to different persons.





Overview of Internal Controls and Risk

Proper authorization of transactions and activities

- Requires the review of transactions by an appropriate person to ensure that all activities adhere to established guidelines, it may be general or specific.
 - For example:
 - Giving a department permission to expend funds from an approved budget
 - general authorization.
 - Review and approval of an individual transaction – specific authorization.



Overview of Internal Controls and Risk

Adequate documents and records

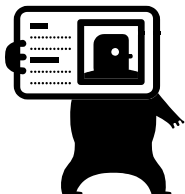
- Provide evidence that financial statements are accurate. The source documents ensure adequate recordkeeping.
 - For example, approved timesheets, payroll reports, etc.



Overview of Internal Controls and Risk

Physical control over assets and records

- The most important measure for safeguarding assets and records is the use of physical precautions – limit access to assets/records
 - Physical Controls – fireproof file cabinets, safe, security cameras
 - Access Controls – passwords, ID cards
 - Backup and recovery procedures – Disaster Recovery Plan





Overview of Internal Controls and Risk

Independent checks on performance

- The need for independent checks arises because internal controls tend to change over time unless there is a mechanism for frequent review.
- For example, edit checks are performed whereby the employee enters their time and the system automatically runs a validation to determine whether enough or too much time has been entered.





Overview of Internal Controls and Risk

Risk is the probability that an event or action will adversely affect the organization.





Overview of Internal Controls and Risk

Identify Risks

- A risk is “what could go wrong” that could lead to a financial misstatement or non-compliance with rules and regulations.
- Risk statements should read as if something went wrong and include the resulting impact (or lost opportunity).
 - Example: Unauthorized changes are made to the payroll master data resulting in payments to fictitious employees and an overstatement of expenses.



Overview of Internal Controls and Risk

Procedure vs. Control:

- A **procedure** is a series of steps taken to accomplish an end.
- A **control** is a series of checks and balances that help managers detect and prevent errors.



Overview of Internal Controls and Risk

- Management uses a mix of **Preventive Controls** and **Detective Controls**
- And a combination of **Manual Controls** and **Automated Controls**



Overview of Internal Controls and Risk

Types and Nature of Controls:

- Prevent - Stop something from going wrong
 - Ex. Approval of timesheets before processing
- Detect - Find and correct errors
 - Ex. Review of payroll summary change reports
- Manual - Performed manually
 - Ex. Comparison of timesheets to preliminary payroll reports
- Automated - Performed by a computer
 - Ex. Access controls to the payroll system

Overview of Internal Controls and Risk

Balancing Risk and Control

To achieve a balance between risk and controls, internal controls should be:

- Proactive
- Value-added
- Cost-effective
- Address exposure to risk





Internal Controls over Payroll Processes

Internal Controls over Payroll Processes

Policies and Procedures



- Describe the organization's leave policies in a personnel manual.
- Establish guidelines for who can view employment records.
- Give access for viewing or updating payroll system data to authorized employees only.
- Provide training for all employees.
- Conduct periodic risk assessments to identify issues.



Internal Controls over Payroll Processes

Payroll Processes

- New Hires and Salary Adjustments
- Terminations (Separations)
- Time Entry
- Payroll Reconciliations

Internal Controls over Payroll Processes

New Hires and Salary Adjustments



- Document approval of budgeted salary and salary adjustments.
- Maintain a personnel file with all relevant employee (*name, address, SS#, birth date, picture ID*) and employment (*salary, withholdings, employment dates*) information.
- Check for completeness and accuracy.
- Segregate human resources and payroll job functions.

Internal Controls over Payroll Processes

Terminations



- Notify human resources and payroll unit when an employee separates.
- Promptly update payroll system and personnel file with date of separation.
- Ensure all time and leave have been entered.
- Segregate human resources and payroll job functions.



Internal Controls over Payroll Processes

Time Entry



- Approve hours worked and leave taken in a timely manner.
 - performed by the employee's supervisor or manager
- Authorize overtime in advance.
- Maintain detail records of leave balances.
- Verify manual timesheets are entered correctly.
- Review exception reports.

Internal Controls over Payroll Processes

Payroll Reconciliations



- Perform reconciliations at least monthly.
- Review and approve all reconciliations.
 - performed by someone other than the preparer



Internal Controls over Payroll Processes

Other Controls

- Monitor payroll records for duplicate names/addresses or postal codes.
- Periodically require employees to pick up paychecks in person with required photo identification.
- Payroll checks should follow controls for cash disbursements.
- Review time entered for holidays.
- Ensure payroll expenses post correctly.



Identifying the Risk


“What could go wrong?”



Identifying the Risk

New Hires and Salary Adjustments

Objectives: Add new employees to payroll system; Make adjustments to existing employees' salaries.

Procedures	Risks “What could go wrong?”	Potential Impact
<ul style="list-style-type: none">• Select job applicant to fill vacant position.• Enter employee information/ changes into payroll system.	<ul style="list-style-type: none">• Salary is entered incorrectly.• Employee exemption status is entered incorrectly.• Fictitious employees are added to payroll.• Employees are paid from the wrong funding source. 	<ul style="list-style-type: none">• Misstatement of payroll expenses and liability accounts• Loss of assets• Payments to fraudulent employees• Compliance issues <p style="text-align: center;">↓</p> <p style="text-align: center;">AUDIT FINDINGS</p>



Identifying the Risk

LACK OF AUTHORIZATION OVER EMPLOYEE PAY RATES

The agency does not maintain adequate documentation for authorization of employee pay rates. During our review, we examined a sample of 60 employees who received a change in salary and identified eight instances where **there was no documented authorization for the change.**

Lack of adequate authorization could result in fictitious employees or employees being paid at unauthorized rates.

Recommendation: The agency should ensure that authorizations for employee pay rates are documented and retained.



Identifying the Risk

PERSONNEL COSTS INCORRECTLY CHARGED TO GRANT

The agency did not have controls in place to ensure that only allowable personnel costs were charged to the Federal grant. Our tests of administrative expenditures revealed that two employees' salaries and benefits were charged to the grant for the entire year even though these employees were not working with this grant. **As a result, funds were expended for unallowable costs.**

Recommendation: The agency should strengthen internal control to ensure that payroll costs are properly charged to grants.



Identifying the Risk

Terminations

Objective: Remove employees from payroll system.

Procedures	Risks “What could go wrong?”	Potential Impact
<ul style="list-style-type: none">• Submit resignation letter/ separation notice.• Calculate leave payout.	<ul style="list-style-type: none">• Separated employees are not removed from payroll system.• Payout is calculated incorrectly.	<ul style="list-style-type: none">• Salary overpayments to separated employees• Overstatement of account balances• Loss of assets <p>↓</p> <p>AUDIT FINDINGS</p>



Identifying the Risk

DEFICIENCIES IN INTERNAL CONTROL OVER SALARY OVERPAYMENTS

The agency has not established or enforced policies and procedures necessary for the effective administration of its personnel processes. As a result, the agency's collection efforts are not in compliance with cash management guidelines.

During our review, we noted **salary overpayments, which remain outstanding, were paid to 10 individuals due to the agency's delayed processing of separation actions.** Our test population consisted of 14 employees whose separation took in excess of 30 days to process. We further noted that collection notices were not sent out in the 15-day intervals prescribed by the agency's cash management plan for those 10 employees that were noted to have been overpaid.

Recommendation: The agency should improve its internal control over salary overpayments to address the deficiencies noted above.



Identifying the Risk

Time Entry

Objective: Record time worked and leave taken.

Procedures	Risks “What could go wrong?”	Potential Impact
<ul style="list-style-type: none">• Enter time worked and leave taken.• Print error reports.	<ul style="list-style-type: none">• Time and leave are not entered or are entered incorrectly.• Time is entered for fictitious or terminated employees.	<ul style="list-style-type: none">• Payment for time not worked• Overstatement of leave balances• Misstatement of payroll expenses and liability accounts• Loss of assets <p style="text-align: center;">↓ AUDIT FINDINGS</p>



Identifying the Risk

INSUFFICIENT CONTROLS OVER TIMESHEETS AND LEAVE BALANCES

The agency does not have adequate monitoring procedures in place to ensure employees' timesheets are reviewed and approved by their supervisors in a timely manner. The payroll system pays salaried employees their full monthly pay rate unless their timesheet indicates otherwise.

Supervisory personnel are responsible for reviewing and approving timesheets to ensure work and leave hours have been properly entered. During our review, we identified 112 employees who had entered time as early as January 2008; however, their **time had not been approved** as of May 2009. We also **identified employees who were paid but had not entered the full amount of hours worked**. As a result, the agency is at risk of paying employees incorrectly and having inaccurate employee leave records. Inaccurate leave records increases the risk of employees taking or being paid for leave that has not been earned.

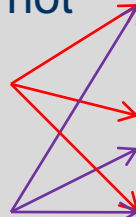
Recommendation: The agency should strengthen its internal control monitoring procedures to ensure payroll and leave balances are accurate.



Identifying the Risk

Payroll Reconciliations

Objective: Identify errors and necessary adjustments.

Procedures	Risks “What could go wrong?”	Potential Impact
<ul style="list-style-type: none">• Agree payroll register total to cash requisition.• Compare payroll to general ledger.• Identify outstanding items and research unreconciled amounts.• Prepare correcting entries.	<ul style="list-style-type: none">• Reconciliations are not prepared or are not timely.• Outstanding or unreconciled items are not researched. 	<ul style="list-style-type: none">• Misstatement of accounts• Loss of Assets• Undetected instances of errors or fraud <p>↓</p> <p>AUDIT FINDINGS</p>



Identifying the Risk

PAYROLL NOT ADEQUATELY RECONCILED

The agency did not complete monthly reconciliations of the total payroll amount processed by the payroll system to the general ledger in a timely manner. In addition, outstanding items were not identified, researched and corrected. As a result, there is an increased risk that a misstatement could occur and not be detected.

Recommendation: The agency should ensure that payroll is properly reconciled each month and outstanding items are researched.



Opportunity for Fraud



Opportunity for Fraud

What is Fraud?

A collection of irregularities and illegal acts characterized by intentional deception, committed by individuals inside or outside of the organization for their personal benefit or to benefit the organization.



Opportunity for Fraud

Fraud Triangle





Opportunity for Fraud

Types of Payroll Fraud

- Ghost employees
- Pay rate alteration
- Unauthorized hours



Opportunity for Fraud

City workers jailed in ‘ghost employee scheme’

Two payroll employees in the city's Department of Solid Waste Management were in jail Tuesday, accused of using a “ghost employee scheme” to steal more than \$144,000 from the city during a two-year period.

Patricia Anita Midell and Bonnie Louise Vital are each charged with theft by a public servant of more than \$100,000, a first-degree felony punishable by life in prison, according to court records.

Assistant Harris County District Attorney Jennifer Devine said Midell, 45, and Vital, 48, **created false employee records by using information from the records of former department employees.**

They deposited checks made out to the “ghost employees” into their own accounts, Devine said. City officials became suspicious after a former employee reported receiving a W-2 for 2008, despite not working for the city.

The former employee initially complained to Vital, Devine said, who told him that she would look into it. After several weeks, he complained to the city controller's office, which alerted the office of inspector general.

City officials said Tuesday the two women no longer work for the city, but requests for start dates and termination dates from the city were not returned Tuesday.

Source: Houston Chronicle <http://www.chron.com/disp/story.mpl/metropolitan/6551107.html>



Opportunity for Fraud

Detroit School Woes Deepen

Five employees of the Detroit public school system were charged Wednesday with multiple felonies as part of an investigation into alleged corruption and the loss of tens of millions of dollars in school funds.

The charges come as the Detroit Public Schools is struggling with an estimated budget deficit of \$259 million and weighing a potential bankruptcy filing.

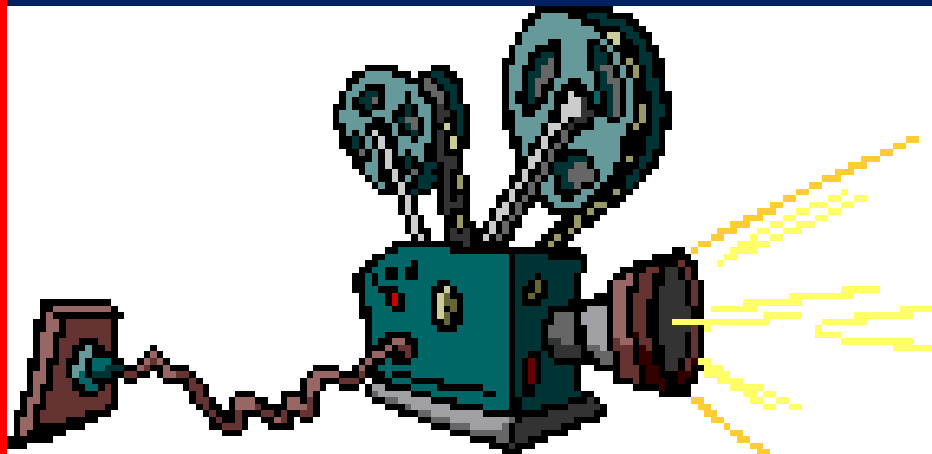
Kym Worthy, the prosecutor for Wayne County, announced the charges Wednesday. If convicted, the accused could face decades of jail time because Michigan law allows harsh penalties for public officials found guilty of wrongdoing.

The losses alleged in the charges represent only a fraction of the improper expenses uncovered since the state sent an emergency financial manager, Robert Bobb, to straighten out the city's ailing school system.

A probe launched by Mr. Bobb uncovered paychecks going to **257 "ghost" employees** who have yet to be accounted for. He said that approximately **500 illegal health-care dependents** he uncovered have cost the district millions. A separate Federal Bureau of Investigation probe in May led to the indictment of a former payroll manager and another former employee on charges of bilking the district out of about \$400,000 over four years.

Source: Wall Street Journal <http://online.wsj.com/article/SB125012223083427629.html>

Opportunity for Fraud



Videos





Opportunity for Fraud

Video links:

New Orleans Police Department video:

<http://www.fox8live.com/news/local/story/Lee-Zurik-Investigation-NOPD-payroll-fraud/damzTLeNw0SFUixBNSiSIA.csp?rss=2085>

Norfolk Community Services Board video:

<http://www.wvec.com/home/Norfolk-employee-paid-for-12-years-of-work-but-never-clocked-in-101564148.html>



Nature of Controls at the Transaction Level

Nature of Controls at the Transaction Level



Significant Accounts / Disclosures in Financial Statements

Classes of Transactions

Business Processes

Process A

Process B

Process C

Financial Applications (application controls)

Financial Application A

Application B

IT General Controls (Activities)

**Manage
Change**

**Logical
Access**

**Other IT
General Controls**

Nature of Controls at the Transaction Level



Nature of Controls at Transaction Level

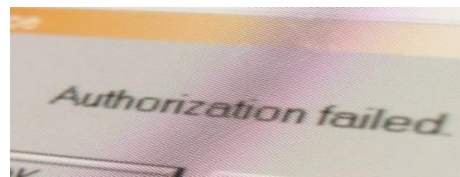
Manual controls are those controls that are manually performed by an individual.



IT dependent manual controls are those controls that manually performed, but require input based upon the results of computer-produced information.



IT application controls are those controls that are performed entirely by a computer or computer-based system.

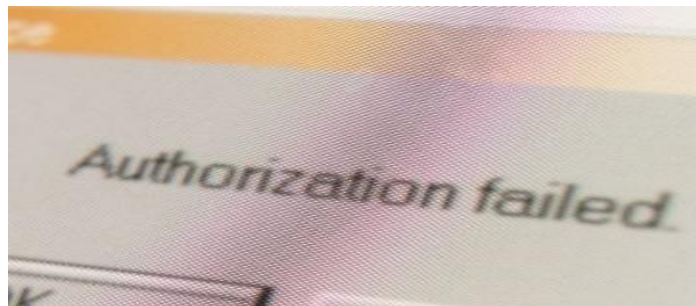


Nature of Controls at the Transaction Level



IT Application Controls are:

- Built into computer programs and supported by manual procedures.
- Designed to provide completeness and accuracy of information processing critical to integrity of the financial reporting process.



Nature of Controls at the Transaction Level



IT Application Controls (input-processing-output)

- Input data is accurate, complete and authorized
- Data is processed as intended in an acceptable time period
- Output and stored data is accurate and complete
- A record is maintained to track data processing from input to storage to output

Nature of Controls at the Transaction Level



IT Application Controls (automated process controls) – Components

- Configuration settings and custom automated controls
- Master data controls and access
- Control overrides
- Segregation of duties and function access
- Interface control

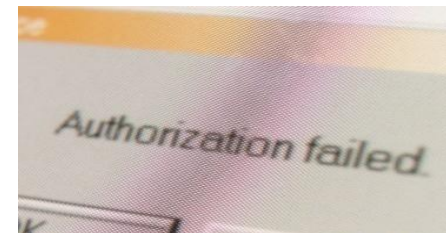
Nature of Controls at the Transaction Level



Common IT Application Controls

Input and access controls

- Data checks and validations
- Automated authorizations, approval, and override
- Automated Segregation of Duties
- Pended Items



File and data transmissions controls



Nature of Controls at the Transaction Level



Common IT Application Controls (cont.)

Processing controls

- Automated file identification and validation
- Automated functionality and calculations
- Audit trails and overrides
- Data extraction, filtering, and reporting
- Interface balancing
- Automated functionality and aging
- Duplicate checks

Output controls

- General ledger and sub-ledger posting
- Update authorization

Nature of Controls at the Transaction Level



End-User Computing

- Generally involves the use of end-user developed spreadsheets and databases.
- It is pertinent that adequate controls are in place for high risk spreadsheets, databases and other user-developed programs as they are equivalent to any other system.
- Example of End-User controls:
 - Access control
 - Version/change control
 - Reviewed for completeness, accuracy and processing integrity
 - Backup

Nature of Controls at the Transaction Level



- IT Application Controls apply to the processing of data within the application software.
- IT General Controls are controls over:
 - Computer Operations
 - System software acquisitions and maintenance
 - Access security
 - Application system acquisition, development and maintenance



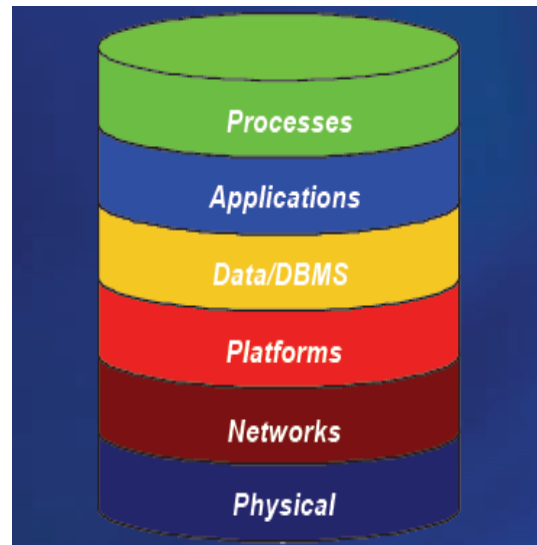
Considering IT General Controls



Considering IT General Controls

Why Should We Consider IT General Controls?

The effectiveness of the application controls is dependent on the general controls.





Considering IT General Controls

Significant Accounts / Disclosures in Financial Statements

Classes of Transactions

Business Processes

Process A

Process B

Process C

Financial Applications (application controls)

Financial Application A

Application B

IT General Controls (Activities)

**Manage
Change**

**Logical
Access**

**Other IT
General Controls**

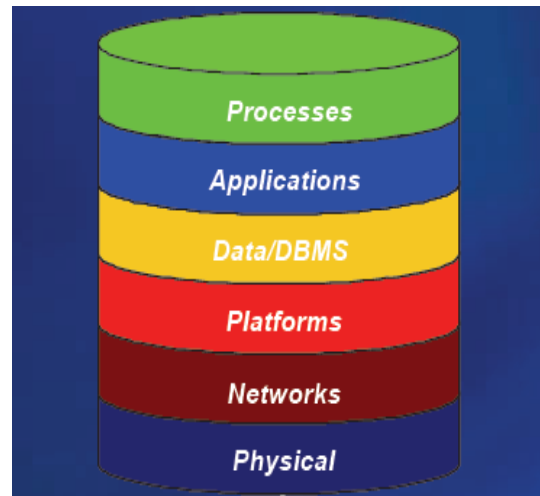


Understanding IT General Controls

Understanding IT General Controls

IT General Controls

- Manage Change
- Logical Access
- Other IT General Controls



Understanding IT General Controls

Manage Change

Only appropriately authorized, tested and approved changes are made to applications, interfaces, databases, and operating systems.





Understanding IT General Controls

Manage Change

- Changes are authorized, tested and approved to confirm application controls operate effectively through the period of intended reliance.
- Changes are monitored on a regular basis for unauthorized changes.



Understanding IT General Controls

Types of Manage Change

- Program Development/Acquisition
- Program Change
- Maintenance to System Software
- Emergency Changes
- Configuration/Parameter Changes



Understanding IT General Controls

Manage Change Controls

Change Management

- Policies and procedures define the changes that required documentation and changes that do not. Significant changes are initiated, approved and tracked.

Change Requests (including emergency changes)

- Supporting documentation is retained in a central repository.
- Appropriate testing is performed depending on the type of change.
- Changes are approved prior to release into production.

Understanding IT General Controls

Manage Change Controls (cont.)

Segregation of Duties

- Between the requesting individual and the approver
- Between developers and those responsible for moving a program change into production
- Monitor program development and changes





Understanding IT General Controls

Manage Change

Objective: Modified, developed or acquired new systems/applications changes.

Procedures	Risks “What could go wrong?”	Potential Impact
<ul style="list-style-type: none">• Change made in the interface between the general ledger and the sub-system.	<ul style="list-style-type: none">• Processing of transactions or data may be incomplete and inaccurate.	<ul style="list-style-type: none">• Misstatement of account balance• Loss of assets <p>↓</p> <p>AUDIT FINDINGS</p>



Understanding IT General Controls

Logical Access

Only authorized persons have access to data and they can perform only specifically authorized functions (e.g., inquire, execute, update).



Understanding IT General Controls

Logical Access (cont.)

- Access to key systems and files is approved, appropriate and monitored to confirm data generated by the application is reliable.
- Application Security – higher level logins and parameter change restrictions confirm applications are secure.





Understanding IT General Controls

Logical Access Controls are applied per the Statewide Security Manual/Agency's Information Security Policy.

These may include:

- Restricted number of sign on attempts
- Automatic password changes
- Minimum length of passwords
- Logging and investigation of unauthorized password events.
- Limited physical access to the data center(s)

Privileged access to system and applications is limited.



Understanding IT General Controls

Logical Access Controls (cont.)

- Users and administrative accounts are not shared between users.
- Periodically review who has access to the critical financial data and configuration settings for the application and systems.
- Anti-virus software is used to protect the integrity and security of financial reporting systems and subsystems.
- Intrusion detection is installed and maintained on critical systems and alerts are actively monitored and addressed.
- Network connectivity is configured to restrict unauthorized access to all network systems.



Understanding IT General Controls

Logical Access and Physical Security

- Access to computer rooms, telephony, networks, power supplies and sensitive IT documentation is granted and revoked by an authorization process.
- Access to computer rooms, telephony, network, power supply cabinets and sensitive IT documentation are controlled with an automated card access system or manual lock.
- Access to computer rooms are documented and logged.
- Access logs are reviewed by IT management and access violations are escalated and resolved in a timely manner.

Understanding IT General Controls

Logical Access Controls

Segregation of Duties related to granting, modifying and removing user access.

- Requesting access, approving access, setting up access and monitoring access
- Access groups/roles are also periodically reviewed for appropriateness and segregation of duties
- Violations/violation attempts
- Performing rights of a “privileged” user and monitoring use of a “privileged” user (password expires every 60 days)





Understanding IT General Controls

Logical Access

Objective: Granting/removing access rights to systems, applications, and data.

Procedures	Risks “What could go wrong?”	Potential Impact
<ul style="list-style-type: none">• Change access rights on previous Personnel Technician.	<ul style="list-style-type: none">• Unauthorized access to the payroll subsystem since her responsibilities have changed.<ul style="list-style-type: none">- Entered ghost employee on the payroll file.- Processing of payroll transactions that are inaccurate.	<ul style="list-style-type: none">• Overstatement of payroll expenses and opportunity for fraud. <p>↓</p> <p>AUDIT FINDINGS</p>

Understanding IT General Controls

Other IT General Controls (computer operations)

- Scheduling
- Backup and Recovery
- Problem Management and Monitoring





Understanding IT General Controls

Scheduling

- Job scheduling and processing procedures

Backup and Recovery

- Backup schedule, offsite storage
- Periodic testing of backup media

Problem Management and Monitoring

- IT operations problems or incidents are identified, resolved, reviewed and analyzed in a timely manner.

Understanding IT General Controls

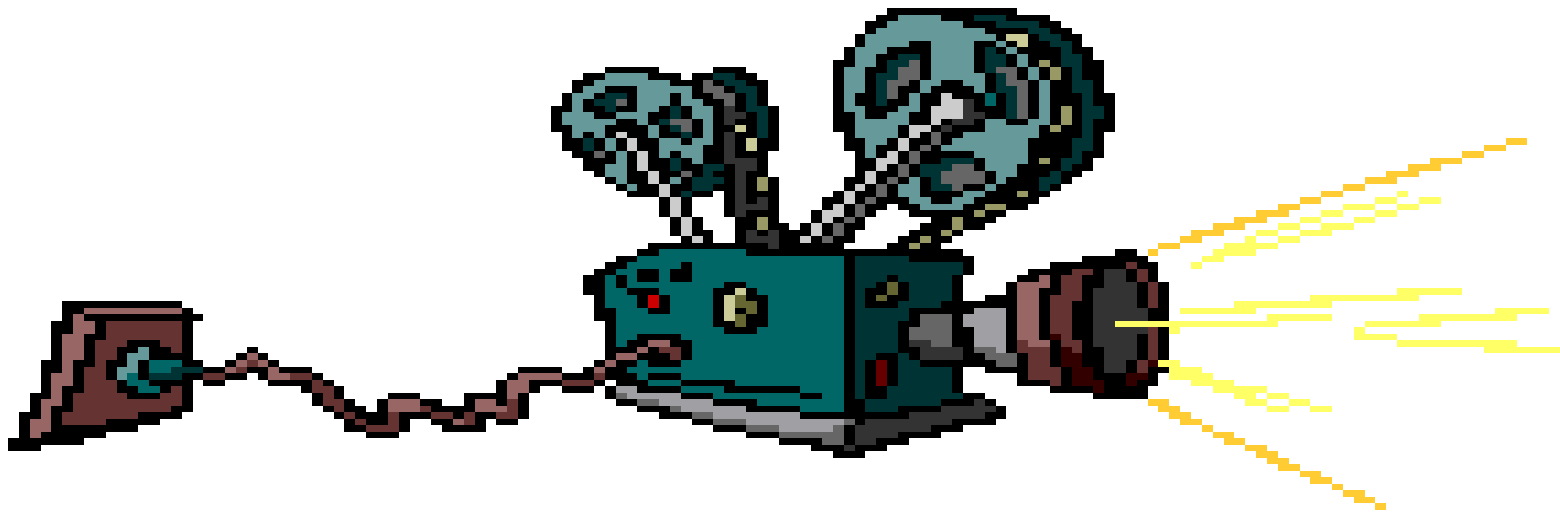
Other IT General Controls (computer operations)

Segregation of Duties of the individuals who

- Perform backups and monitoring
- Program and implement/monitor scheduling



How IT General Control Weaknesses Could Lead to Fraud?



Videos

How IT General Control Weaknesses Could Lead to Fraud?



Video links:

Student Hacks Computer to Change Grades:

<http://www.youtube.com/watch?v=zTEwALs1i3g>

University of Louisville Database Breach:

<http://www.youtube.com/watch?v=ZoApF5pCxpI>



Key Take-Aways



Key Take-Aways

What is an Internal Control?

- An action taken to mitigate or manage risk that increases probability that an organization's processes will achieve its goals/objectives.
- Provides the foundation for accountability
- Helps organizations detect/prevent problems.



Key Take-Aways

Examples of Internal Control Activities:

- Adequate segregation of duties
- Physical control over assets and records
- Proper authorization of transactions



Key Take-Aways

What is Risk?

- The probability that an event or action will adversely affect an organization.

Risk Identification

- Determine “what could go wrong?”
- Assess potential impact resulting from something going wrong.

Key Take-Aways

Balancing Risk and Control

To achieve a balance between risk and controls, internal controls should be:

- Proactive
- Value-added
- Cost-effective
- Address exposure to risk.





Key Take-Aways

Internal Controls over Payroll Processes:

- New Hires and Salary Adjustments
- Terminations (Separations)
- Time Entry
- Payroll Reconciliations



Key Take-Aways

Types of Commonly Seen Payroll Fraud:

- Ghost Employees
- Pay Rate Alterations
- Unauthorized Hours



Key Take-Aways

Controls at the Transaction-Level:

- Manual Controls
- IT Dependent Controls
- IT Application Controls



Key Take-Aways

Categories of IT Application Controls:

- Input and Access Controls
- Processing Controls
- Output Controls

Provides assurance of transaction:

- Completeness
- Accuracy
- Validity



Key Take-Aways

IT General Controls

- Manage Change
- Logical Access
- Other IT General Controls (Computer Operations):
 - Scheduling
 - Back-up and Recovery
 - Problem Management and Monitoring



Thank You!